Maricopa County
Office of Enterprise Technology
Information Security Handbook

What you need to know to stay safe while computing, and help protect the county's IT assets.

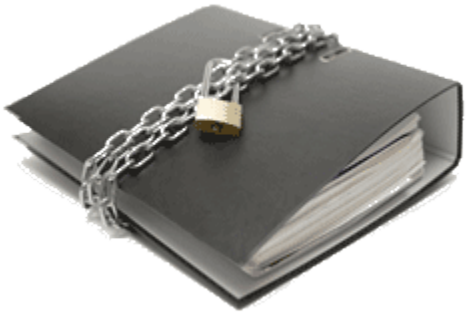
Please contact the Customer Resource Center to inquire about Information Security Issues.
602-506-HELP or email at helpdesk@mail.maricopa.gov

Table of Contents

Introduction

Whether you realize it or not, you and your co-workers are critical to protecting information at Maricopa County. You are on the front line daily and play a key role in the overall security strategy.

This handbook will provide you, the Maricopa County employee or elected official with the basics needed to help you protect the County's Information resources. Maricopa County provides a wide range of electronic equipment, systems and software for you to use to communicate, store and process information. These include: desktop computers, laptops, mainframes, software, networks, email, instant messaging, internet access and smart phones to mention just a few.



While Maricopa County Security Policies, Standards and Guidelines cover all County agencies and describe various security related issues in detail, this handbook focuses on the very basic and minimal information needed to help you protect your organization's information assets.

Twelve things you can do to protect the County's assets

1. **Become familiar with the county's information technology security and privacy policies**
   Policies, standards and guidelines are developed to protect the County's information and information assets from loss, damage, destruction or tampering from unauthorized users.

2. **Manage protected information properly**
   Always be thoughtful of the damaging nature of information to which you have access and protect it appropriately. Do not leave paper documents, files or electronic media containing protected information where an unauthorized person can see or obtain it.

   Protected information is defined in Maricopa County policy as:

   "Social security number; date of birth; mother's maiden name; state driver's license number; state identification card number; federally issued identification number(s); health care information; bank account or other financial information about individuals or businesses; and any information, or combinations of information, the disclosure of which could compromise the security of county functions."

3. **Choose your password wisely and keep it secure**
   Your login name and password (collectively called authentication credentials) identify you to systems and applications to which you have access on the County network. **You are responsible for protecting your password from getting into the wrong hands.**

At Maricopa County, you are required to change your password every two months (60 days). Your new password must be unique. You must use at least eight (8) upper and lower case letters, numbers, and certain symbols. The system will not allow passwords that are similar to previously used passwords.

Policy: Can be thought of as the laws of the organization. They are a set of organizational rules and practices that regulate how an organization manages, protects and uses its information assets. Policies must be followed. Any exceptions to policies must be documented, reviewed and approved.

Standard: Rules indicating how and what kind of software, hardware, databases, protocols, and business processes must be implemented, used and maintained to meet policy objectives. Standards also must be followed. Any exceptions to standards must be documented, reviewed and approved. Standards are based in part on technology, and as technology changes, standards may need to be updated.

Guideline: Recommended actions and/or industry best practices used to guide Maricopa County practices by users, IT staff and others. Guidelines are not compulsory. Guidelines are based largely on the technologies used, therefore, guidelines may change as frequently as technology changes.

4. Understand social engineering

We often think of computer security and privacy as technical in nature, but in reality the weakest part of any computer security system is people. Social engineering is a form of a con-game, where an attacker attempts to trick or mislead someone in order to gain access to protected information with the intent of using that information or access to compromise a system. Examples of social engineering include:

- Someone persuading an employee to let them through a security door.
- An attacker pretends to be an IT staff member and asks an employee for a password.
- An attacker sends an email to trick an employee into entering protected information into their website. This form of attack is generally used to steal user names and passwords from unsuspecting employees.

Another form of social engineering is 'shoulder surfing'. Shoulder surfing is when someone tries to figure out passwords, or read documents, by looking over your shoulder. Make sure your monitor is not easily viewed by other walking by your desk.

5. Use and protect smart phones and other consumer devices securely

Smart phones (such as iPhones, Blackberries™, Windows Phones, etc.) and other consumer devices (such as iPads, Android pads) are important tools enhancing availability and productivity for County employees. These devices also access County information such as

Email & IM Safety Tips

- *Do not open an email attachment or file unless you know who it's from. Save attachments to your hard drive to allow the antivirus program to scan it before opening.*
- *Do not click on a link unless you know who sent it.*
- *Keep antivirus software up to date. If you think your computer is not updating automatically, contact the Customer Resource Center at 602-506-HELP or by email at helpdesk@mail.maricopa.gov.*
- *Do not forward any type of security, informational, or virus warnings. Report it to your IT support or the Customer Resource Center at 602-506-HELP or by email at helpdesk@mail.maricopa.gov.*
- *Know how to deal with email spam and hoaxes. If you receive an email message that you believe is a hoax, take the time to check the facts. For hoax information, visit:* https://www.dhs.gov/internet-hoaxes. *Delete the message or forward to* informationsecurity@mail.maricopa.gov *or the Customer Resource Center at 602-506-HELP or by email at helpdesk@mail.maricopa.gov.*
- *Beware of spoof email claiming to be from a company you trust asking for personal information. This is called phishing. The email may inform you that there is a problem with your account/password. There may be a link to click. Forward any of these emails to the company it claims to be sent from (each organization usually provides an "abuse" email address on their webpage). Reputable organizations like Yahoo!, MSN, Gmail or your bank will never ask you for your email password. Don't fall for it.*
- *Make sure to disable Outlook attachment previews. Attachment previews takes away your ability to decide whether or not to open an attachment.*

email and may have some availability to files and systems. People often make the mistake of thinking these devices do not need security. On the contrary, they need just as much security as a PC. Smart phones and other consumer devices are as powerful and functional as personal computers; however, they are smaller, mobile and easily lost, misplaced or stolen. Whether or not your smart phone or other consumer device is your own personal property or assigned to you by the County, if you are storing county information on it, **you are responsible for ensuring the data is secure.** You should always use passwords and encryption, when available. You must always be wary and prevent its loss or theft, and if it is, arrange to remove the data in a secure manner immediately and before you dispose of it. Be aware of the fact that much of what has been mentioned here also applies to laptops and removable media such as USB drives.

6. Keep equipment and data secure when working remotely

Remote computing, (often referred to as Telecommuting), allows you to do business outside of the traditional office. It takes place when you are away from the office and using computer equipment to conduct County business. Reasons for remote computing include such things as working from home, a hotel, airport, or other location. Receiving or sending email while away from the office is also considered remote computing.

You are subject to the same County policies regarding the use of County provided hardware, software, and services when working remotely as you are at work. You must follow the County's software standards and policies. Do not let anyone, except County employees, use County provided hardware, software, or services when you are traveling or at home.

7. Know the risks associated with email and instant messaging

Email and instant messaging (IM) are an essential part of Maricopa County's communication tools. Attachments and embedded links in email can be a major source of malware infections or social engineering. It is important to know how to safely deal with email and instant messages in order to protect the county's assets from compromise.

8. Use the Internet safely

The Internet has a wealth of information and resources for business and personal uses but it also is a source for inappropriate content and malicious software. Use the Internet as if you were being observed. Some examples of prohibited, non-business sites include any that contain:

- Adult content
- Racist, chauvinistic or defamatory

- Gambling oriented
- Personal chat rooms

When signing up for, installing or agreeing to anything, read the fine print. If you do not want to receive junk mail or get put on a telemarketer list, look for a box usually near the bottom of the page that asks if you want to receive information and offers, this is called "opting out". Most companies assume you want to "opt in", so the box will likely be checked, read the information carefully and select appropriately for you. The best sites will have a privacy policy regarding your information and what they do with it. Some sites require you to give all your information to get the product or service they are offering. Only provide the information that indicates "required".

Do not give out your full name, address, or phone number to anyone online that you don't trust or know personally. This is especially important in chat rooms. Beware of mass distribution letters (i.e. very general emails that don't actually address you personally), anyone who wants to negotiate a wire transfer, or anyone who wants to work out a business arrangement while they're abroad, including your friends.

Social Networks:

Social networking is everywhere. With social networks, people across the world have access to tools and options that were previously non-existent. However, there are just as many opportunities to connect with others as there are potential dangers. Social networking has opened up many new doorways for cyber-crime, and with all the people on social networks who are new to technology, it is more important than ever to make sure you are aware of the risks.

Phishing/Scams – There are a number of scammers on social networks who may try to steal or use your personal information. Information that can be used for potential crime such as identity theft or fraud. Once someone has your password, they can use it to destroy your profile or send out spam messages and viruses. This could do irreparable damage to your online reputation, not to mention, your financial one.

Always make sure you are at the right web site when you enter your credentials. You can do this by double checking the address bar and making sure you are in the right place before you log in.

Privacy – Many people are wary of uploading their photos or videos to a social networking site, like Facebook, because they are concerned about retaining ownership. There is a major gray area as to who would own the material(s) that is uploaded. Only upload those items that you do not care about retaining original ownership.

Employment – One thing we often forget while having fun on social networks is that almost anybody can see what we are doing. While we are tagging photos of what we did on the weekends, or tweeting our thoughts, it can be easy to forget that someone at work or potential employers may see this and the result could cost you.

Businesses – Organizations have found a new place to market and brand themselves in social media sites. Having a medium available to connect with customers in a non-formal way creates loyalty and awareness, but could leave an organization vulnerable to hackers and hecklers.

Acceptable Use of the Internet:

Never download or install software unless you get specific approval ahead of time. Do not visit chat rooms using Maricopa County's resources.

As discussed under the section on email security, only download files or software from sites that have been rated or verified by trusted sources. Choose downloading resources that are up-front about price and ratings, and examine the download (i.e. download.cnet.com). When in doubt, Google the name of the site or download along with the word "scam" to see if you get any results.

Secure Transactions:

Always make sure that online transactions are secure. The best web sites will have many security devices in place. You may see a gold lock on the page to indicate a secure site. When giving any bank details, login information or any other personal information, make sure the connection is secure (URLs like this begin with HTTPS:// instead of HTTP://) and the site is trustworthy.

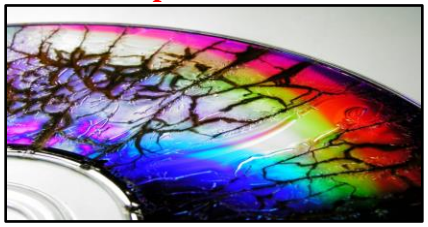
Secure Workspaces

- Treat protected information like any other type of valuable. Lock up physical files and media such as hard copy files, CD-ROM, USB drives, etc.
- Make sure your monitor is not easily viewed by people walking by your desk.
- Use screen saver passwords – this will password lock your computer when it is idle for a period of time. You can immediately lock your screen by pressing the Windows key (⊞) and the "L" key simultaneously.
- Use laptop cable locks to protect against theft.
- Always maintain a clean and uncluttered desk.

9. Secure work spaces when away

Securing your work space means that when you are not at your desk, protected information is properly locked and secured against unauthorized access.

10. Back-up and secure data when not on the network



We all take for granted that the hard drives in our computers and USB drives will always be reliable and available. Unfortunately, most of us do not take the time to back up our data as frequently as we should. We strongly recommend that you store your files on one of the county's servers, not solely on your local hard drive or

removable media (USB drives). By keeping copies of your files on a server, you ensure that your information is backed up regularly by the IT department. This also adds an additional layer of security to your data because servers are located in physically secured facilities and physical access is limited to those who have the proper security and authority.

11. Dispose of digital media safely

It's simply not enough to just 'delete' a file. Deleting data does not actually remove the files from the drive. To permanently delete information, you must use special hardware and/or software.

12. Know what to do when things go wrong

Is your PC acting funny, not working the way you are used to? Something has probably changed on your PC or the network. This could be a result of an incident, patches that were deployed or some other factor. What do you do in this case? First of all stay calm, do not try and fix the problem or handle the incident, yourself. Contact the Customer Resource Center at 602-506-HELP or by email at helpdesk@mail.maricopa.gov. They will troubleshoot and initiate the proper procedures for addressing the problem.

As a Maricopa County employee, you are responsible for following the policies and understanding the laws that govern your work. You are responsible for taking the appropriate actions to make sure Maricopa County assets are protected.

How to Dispose of Digital Media (after record retention considerations)

- USB drives should be erased and crushed. Dispose of the parts in several trash receptacles.
- CDs and DVDs can be run through a CD shredder, industrial paper shredder, or placed in a microwave for 3 seconds. This produces an interesting light show, destroys the media but does not harm the microwave.
- Computer hard drives should be wiped using special software and/or hardware by the IT department before disposal or surplus. This is especially important for drives from servers being decommissioned.

Glossary

Acceptable Use: The conduct expected from a person using a computer or service.

Appropriate Use: Distinguished from Acceptable use in that appropriate is suitable or fitting for a particular purpose, person, occasion or circumstance.

Asset: Anything of value to an organization. Assets can include computer rooms, networks, digital and paper records, hardware, software, people, and data.

Authentication: A security procedure designed to verify the validity of the authorization credentials entered by a user to gain access to a network or system.

Authentication Credentials: The combination of login (user ID) and password.

Authorization: The right or permission to use a system resource.

Availability: Ensuring that authorized users have access to information and associated assets when required

Backup: Duplicate copies of data on different storage media created for emergency and recover purposes.

Breach: The unauthorized disclosure of information that compromises the security, confidentiality, or integrity of personally identifiable information.

Confidentiality: Ensuring that information is accessible only to those authorized to have access.

Control: A means of managing risk, including policies, procedures, guideline, practices or organizational structure which can be of administrative, technical, management or legal nature. Often synonymous with safeguards or countermeasures.

Data: Distinct pieces of information, which can exist in various forms such as numbers, text, bit, bytes, or memory.

Disclosure: Revealing stored or protected information. Laws and organizational procedures define the circumstances under which information is disclosed or protected from disclosure.

Eliminate: To completely remove a threat or vulnerability from the environment reducing the probability of it being exploited to zero.

Encryption: The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Email: Electronic mail are messages and any attachments that are sent by means of electronic mailing systems such as Microsoft's Exchange or the email provided by most Internet service providers.

Guideline: Recommended actions and/or industry best practices that should be used to guide Maricopa County practices by users, IT staff and others. Guidelines are not compulsory. Guidelines are based largely on the technologies used therefore guidelines may change frequently as technology changes.

Hacker: Someone who creates and modifies computer software and computer hardware including administration and security-related items; typically thought of as a person who illegally gains access to and sometimes tampers with information in a computer system.

Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Information: The combination of pieces of data producing meaningful and usable output.

Information Asset: A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization that has one or more of the following characteristics: Not easily replaced without cost, skill, time, resources, or a combination' Part of the Organization's identity, without which, the Organization may be threatened.

Information Assurance: Information Assurance (IA) is the practice of managing information-related risks. More specifically, IA practitioners seek to protect the confidentiality, integrity, and availability of data and their delivery systems. Information Assurance is closely related to information security and the terms are sometimes used interchangeably. However, IA's broader connotation also includes reliability and emphasizes strategic risk management over tools and tactics. In addition to defending against malicious hackers and code (e.g., viruses), IA includes other corporate governance issues such as privacy, compliance, audits, business continuity, and disaster recovery. Further, while information security draws primarily from computer science, IA is interdisciplinary and draws from multiple fields, including fraud examination, forensic science, military science, management science, systems engineering, security engineering, and criminology, in addition to computer science. Therefore, IA is best thought of as a superset of information security.

Information Custodian: The person who is responsible for defining specific control procedures, administering information Access Controls, implementing and maintaining cost-effective information control measures, and providing recovery capabilities consistent with the instructions of Information Owners.

Information Owner: The person who is responsible for protecting an Information Asset, maintaining the accuracy and integrity of the Information Asset, determining the appropriate Data sensitivity or classification level for the Information Asset, reviewing its level for appropriateness, and ensuring that the Information Asset adheres to policy.

Information Security: The business process designed to manage risks to the confidentiality, integrity and/or availability of the organizations information assets.

Information System: Software, hardware and interface components that work together to perform a set of business functions.

I**nformation Privacy:** Ensuring that individuals maintain the ability to control what information is collected about them, how it is used, who has used it, who maintains it and what purpose it is used for as provided within the law.

Integrity: Safeguarding the accuracy and completeness of information and processing methods.

Internet: A global set of interconnected smaller networks that transfer data. It is a "network of networks" that consists of millions of smaller domestic, academic, business, and government networks, which together carry various information services.

Internet Mail: Electronic mail sent or received over the Internet.

Maricopa County Information Privacy Policy: A policy that governs the collection and use of personal information. It also acknowledges that while Maricopa County information is generally available for public review, the county is committed to protecting personal information contained in its records.

Laptop: A small mobile personal computer usually weighing from two to six pounds (also known as a laptop computer, notebook computer, or notebook).

Least Privilege: Granting a user only those access rights needed to perform official job duties.

Logic Bomb: Programming code, inserted surreptitiously or intentionally, designed to execute (or "explode") under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a command. A delayed-action computer virus or Trojan horse. A logic bomb, when "exploded," may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects. Synonymous with slag code.

Login: A unique code or string of characters used to identify a specific User. Often referred to as User ID, Login Name or Login ID.

Malware: Malicious software designed to destroy, aggravate and otherwise make life unhappy. See virus, worm, logic bomb and Trojan horse.

Minimal Personal Use: Use that is brief in duration and frequency, and does not interfere with or impair the conduct of official county business, and results in negligible or no expense to the county.

Mitigate: Something that lowers the probability of a vulnerability or threat being exploited. For example, installing intrusion prevention can mitigate the spread of worms. Note that mitigation is not the same as elimination. When a threat is mitigated, the probability is merely reduced (preferably to a very low probability).

Organization: Every county office, every officer, every institution, whether educational, correctional or other, and every department, division, board and commission.

Passphrase: An exceptionally long password generally derived from a phrase or short sentence that typically eliminates spaces and replaces some letters with special characters; for example "TheDark3stHourI$JustBeforeDawn". (Do not use this example.)

Password: A confidential sequence of characters used to authenticate an individual's identity, usually during a logon process.

Personally Identifiable Information (PII): Any information concerning an individual which is contained in an Organization record and, because of name, identifying number, image, mark, or description, can be readily associated with a particular individual, including information contained in printouts, forms, written analyses, or evaluations.

Policy: Set of countywide organizational rules and practices that regulate how an organization manages, protects and uses its information system assets and data. These are required and must be complied with. Any exceptions to these must be documented, reviewed and approved. Policies are reviewed only when business operation changes dramatically.

Protected Information: Social security number; date of birth; mother's maiden name; state driver's license number; state identification card number; federally issued identification number(s); Health Care Information; bank account or other financial information about individuals or businesses; and any information, or combinations of information, the disclosure of which could compromise the security of county functions.

Risk: The combination of the probability of an event and its consequences.

Risk Assessment: Assessment of the threats to, impacts on and vulnerabilities of information assets and the likelihood of their occurrence

Risk Management: The process of identifying, controlling and minimizing or eliminating security risks that may affect information system, to an acceptable cost**.**

Risk Treatment: The process of selection and implementation of measures to modify risk.

Safeguard: A mechanism (software, hardware, configuration, etc.) that protects. For example, a firewall is a network security safeguard.

Security: An attribute of information systems which includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services and the privacy of individuals.

Security Control: Technical or non-technical process employed by an Organization to protect information systems, detect breaches in its information security, and mitigate information security risks.

Sensitive Information: Any information that is protected from public disclosure or information whose disclosure, misuse, loss or unauthorized alteration could harm the County, an Individual, Service Provider, or other Third Party. Sensitive information may be subject to public.

Standard: Rules indicating how and what kind of software, hardware, databases, and business processes must be implemented, used and maintained to meet policy objectives. Standards are required and must be complied with. Any exceptions to these must be documented, reviewed and approved. Standards are based in part on technology and as technology changes, standards may need to be updated.

Strong Password: A password that consists of combination of upper and lower case letters, numbers and special characters; sometimes referred to as a "complex password".

System: Software, hardware and interface components that work together to perform a set of business functions.

System Administrator: The person assigned to manage and maintain a specific system. This individual usually has elevated rights and privileges on the specific system.

System Password Policies: Password policies that relate to a specific system. Due to technological limitations of specific systems, special password policies must be developed to ensure secure authentication.

Threat: A potential to cause an unwanted incident which may result in harm to any or all information assets. Threats could be intentional or accidental.

Trojan horse: A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can take control and perform its programmed form of damage.

URL: Abbreviation of Uniform Resource Locator *(URL)* it is the global address of documents and other resources on the Internet. URL is Synonymous with Web Address.

USB flash drive: A data storage device that integrates with a USB (Universal Serial Bus) interface. It is typically small, lightweight, removable, and rewritable; also known as a thumb drives or jump drives

User: Any individual performing work for Maricopa County utilizing a personal computer, workstation, laptop or terminal, including but not limited to any employee, contractor, consultant, or other worker. Each term is used in the general sense and is not intended to imply or convey to an individual any employment status, rights, privileges, or benefits.

User-Id: A unique code or string of characters used to identify a specific User. Often referred to as Login.

Virus: A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Most viruses can also replicate themselves and spread to other computers. All computer viruses are man-made.

Vulnerability: A weakness in an organizations information security, in itself does not cause harm it is a condition or set of conditions that may allow a threat to affect an asset.

WAN: Wide Area Network - A computer network covering a broad geographical area.

Web Browser: Software used to access and navigate the World Wide Web.

Wireless network: A wireless network is a computer network consisting of wireless access points (WAPs) that uses radio waves, rather than physical wires, to connect laptops, PCs, and PDAs to a network.

Workforce Member: Employees, volunteers, and other persons whose conduct and, perform work for Maricopa County, are under the direct control of Maricopa County, whether or not they are paid by Maricopa County. This includes full- and part-time elected or appointed officials, members of boards and commissions, employees, affiliates, associates, students, volunteers, and staff from third-party entities who provide service to Maricopa County.

Worm: A worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

World Wide Web: A major service on the Internet. The World Wide Web is made up of "Web servers" that store and disseminate "Web pages," which are "rich" documents can contain text, graphics, animations and videos to anyone with an Internet connection. The heart of the Web technology is the hyperlink (the "URL"), which connects each document to each other, whether locally or around the world by clicking a link.